# RANSOMWARE DEFENCE STRATEGIES: DVANCEMENTS, CHALLENGES AND FUTURE PROSPECTS

**Vinson Jos Kunnankada** FPM Scholar, ISBR Business School, # 107, Near INFOSYS, Behind BSNL Telephone Exchange, Electronic City - Phase I, Bangalore - 560 100

Email-vinson.fpm2021@isbr.in

FPM guide-Dr. Naveen Pol(Associate Professor, ISBR Business School, Bangalore)

**Abstract:**

This research paper delves deeply into the escalating threat posed by ransomware attacks, necessitating a comprehensive examination of defence strategies. It scrutinizes both established and emerging tactics for combating ransomware, drawing insights from real-world case studies, technological advancements, and collaborative defence frameworks. The study explores the evolving landscape of ransomware tactics, assesses the effectiveness of traditional defence measures, and explores cutting-edge strategies being developed. It emphasizes the pivotal roles of AI and machine learning in enhancing detection and response capabilities, resilience planning to minimize impact, and robust incident response protocols. Additionally, the paper speculates on future trends and potential innovations in the ongoing battle against ransomware adversaries. Through these analyses, it aims to provide organizations with actionable insights to strengthen their defences and resilience against ransomware assaults.

Ransomware attacks have seen a dramatic rise in both frequency and complexity, presenting significant challenges to organizations globally. The escalating number of cyber-attacks, specifically ransomware incidents, is alarming due to their potential to compromise users' device integrity and data security. These attacks typically involve either locking the user's device screen or encrypting their files, demanding payment of a ransom for restoration. This trend highlights a growing threat landscape where ransomware attacks have become more pervasive and detrimental in their impact.

The consequences of ransomware attacks are profound and can endure long after the initial incident, with data recovery often proving difficult even after the ransomware itself is eradicated, necessitating intervention from the attacker. Despite these challenges, recent advancements in Situational Awareness (SA) and cognitive methodologies have significantly enhanced the ability to swiftly detect ransomware threats.

By fortifying detection mechanisms and deploying proactive prevention strategies, objective is to reduce the aftermath of ransomware attacks and enhance the protection of user data. Through collaborative initiatives and continuous research, strivings to anticipate and counter evolving ransomware threats effectively, thereby bolstering defences against cyber-attacks for the long term.

**Introduction**:

In modern times, ransomware attacks has turned into a widespread and severe cyber threat, causing significant financial losses, operational disruptions, and data breaches globally. Cybercriminals continually refine their tactics with advanced encryption and new attack methods, challenging organizations to defend against these evolving campaigns effectively. This dynamic landscape requires robust cybersecurity strategies, including threat intelligence, continuous monitoring, data backups, and employee training, alongside collaborative efforts across sectors to mitigate risks and protect against ransomware threats.

This research paper explores the vital area of ransomware defence strategies, analysing recent advancements, organizational challenges, and future prospects for combating this pervasive cyber threat. Ransomware attacks involve encrypting an organization's data and demanding payment for the decryption key. Victims must choose between paying the ransom and risking data loss while attempting recovery.

The increasing sophistication of ransomware attacks has surpassed traditional defence mechanisms, making conventional cybersecurity measures ineffective against these highly targeted and adaptive threats. Signature-based antivirus solutions and perimeter-based security measures, which were once considered strong defences against cyber intrusions, have proven inadequate in keeping up with the rapid evolution of ransomware tactics.

This research endeavours to investigate advanced technologies and strategies that show potential for enhancing ransomware defences. Approaches such as behaviour-based detection, sharing threat intelligence, deploying deception technologies, and other innovative methods have emerged as promising solutions to combat ransomware. By implementing proactive and dynamic defence measures, organizations can improve their ability to detect and mitigate the impact of ransomware attacks effectively.

However, organizations encounter complex challenges in effectively defending against ransomware. The attack surface is growing because of the widespread adoption of cloud computing, IoT devices, and secluded work setups, which provide more avenues for ransomware attacks to

exploit. Additionally, there is a global shortage of skilled cybersecurity professionals, compounded by budget limitations, further stretching organizations' capacity to implement strong defences.

In this research, delving into real-world case studies of organizations will be done that have effectively defended against ransomware attacks. Through detailed analysis of these cases, our goal is to glean valuable insights into the strategies, technologies, and incident response protocols that bolstered their resilience against ransomware. Additionally, collaborative defence frameworks have surfaced as a promising strategy in combating ransomware. Public-private partnerships and initiatives for sharing threat intelligence can enhance organizations ability to reinforce their protection and reduce the impact of prevalent ransomware tactics.

In the future, this research paper will investigate emerging trends and prospects in ransomware attacks and defence strategies. The combination of artificial intelligence and machine learning holds the potential to revolutionize ransomware detection and response capabilities, offering organizations the opportunity to proactively stay ahead of cyber adversaries.

In conclusion, ransomware attacks have evolved from a minor inconvenience to a serious and widespread threat, demanding a proactive and comprehensive defence approach. This research paper has explored advancements in ransomware defence, analysed real-world case studies, and envisioned future prospects to equip organizations with the knowledge and strategies necessary to enhance their resilience against ransomware. By adopting these insights, organizations can better safeguard their invaluable digital assets against this persistent cyber threat.

**Problem Statement**

The WannaCry and Petya ransomware attacks represent pivotal events in the cybersecurity landscape, profoundly affecting both businesses and individuals worldwide. These incidents enhance the critical need for strong cybersecurity steps and proactive defences against evolving threats. The widespread impact of WannaCry and the destructive capabilities demonstrated by Petya highlight the imperative for organizations to prioritize comprehensive security measures. This includes regular software updates, effective patch management practices, and thorough employee training initiatives. These proactive steps are critical in blocking and reducing the impact of ransomware attacks, safeguarding organizational systems and data against evolving threats.

Absolutely, the rise of ransomware attacks like Petya, which may have political motivations, underscores the multifaceted nature of cybersecurity challenges. These incidents not only target financial gain but also can disrupt critical infrastructure and sow political discord. Addressing such threats requires concerted efforts from governments, law enforcement, cybersecurity experts, and private industries. Collaboration is crucial for sharing intelligence, developing effective responses, and implementing preventive measures to safeguard against future attacks. This collective approach helps in mitigating the impact of cyber threats and enhances overall cybersecurity resilience on a global scale.

Moving forward, it is essential for both businesses and individuals to maintain vigilance and implement comprehensive defence strategies in order to effectively combat ransomware and other cyber threats. This includes raising awareness and providing training on the current phishing methods, safe browsing habits, and how to identify dubious activities. Keeping all software up-to-date with the latest security patches is critical to prevent misuse of known sensitivities by cybercriminals. Setting up a robust data backup plan that includes regular, secure offline backups confirms that data can be restored without resorting to paying ransom in the event of an attack. Executing network distribution and strong access controls helps limit the advance of malware within systems and restrict unapproved access. Developing and frequently testing an incident response plan ensures quick identification, response, and recovery from ransomware incidents, enabling effective containment, mitigation, and restoration measures to be swiftly implemented. Collaboration with industry peers, cybersecurity experts, and law implementation organisations for details sharing and be aware of emerging threats is also vital. Investing in advanced cybersecurity solutions such as endpoint and intrusion detection along with  response enhances the capability to monitor and respond to threats practically. By taking these dynamic steps, organizations and individuals can outstandingly bolster their defences against cyber threats in an ever-evolving digital landscape.

**Scope of the Study**:

This study presents a comprehensive overview of ransomware analysis techniques, which are classified into three main types: static, dynamic and hybrid. Static study involves examining ransomware executables without executing them, focusing on file structure, metadata, and embedded resources to detect potential indicators of compromise. Dynamic study, on the other hand, involves implementing ransomware in a managed environment like a virtual machine to notice real-time behaviour such as file system changes, registry modifications, and network communications. Hybrid analysis combines aspects of both static and dynamic approaches, leveraging initial static insights to inform and enhance dynamic analysis results. These techniques are essential for gaining deep

insights into ransomware behaviour, supporting the development of effective defence strategies, and bolstering cybersecurity resilience against evolving ransomware threats.
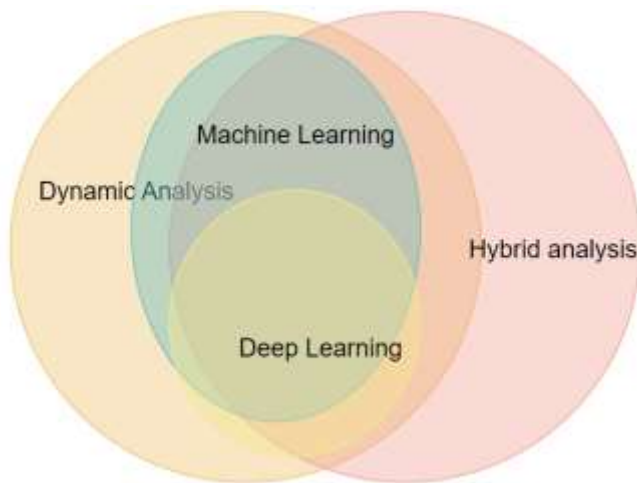


Static study involves inspecting ransomware characteristics without implementing its code, comparing features with a repository of known malicious code. Dynamic study, on the other hand, require actively executing ransomware in a controlled environment to observe its behaviour, monitoring API calls, network activities, and system interactions. Hybrid Analysis integrates both static and dynamic approaches to enhance accuracy by leveraging their respective strengths.

The study explores various research endeavours that employ machine learning, deep learning, or a union of both for ransomware detection. Machine Learning Approaches utilize algorithms to analyse features extracted from ransomware behaviour, such as system calls or network traffic patterns. Deep Learning Approaches apply techniques like LSTM or auto encoders to detect ransomware based on its behavioural patterns. Hybrid Approaches that combine machine learning and deep learning aim to maximize detection accuracy by harnessing the complementary strengths of both methodologies. These advanced techniques contribute significantly to improving cybersecurity defences against ransomware threats in today's complex digital landscape.

The study underscores several key limitations and challenges in ransomware detection. Evasion Techniques, such as obfuscation or encryption mechanisms, are frequently employed by ransomware developers to avoid detection. Static Analysis, while valuable, often suffers from higher false alarms and limited accuracy compared to Dynamic Analysis, which observes ransomware behaviour in real-time. Dataset Limitations in some studies, including insufficient details on sample size and sources, can hinder robust analysis. Short Analysis Timeframes may allow ransomware samples to evade detection, and there are also concerns about the potential compromise of Runtime

Detection programs by malicious software. Hardware data collected during analysis could also be corrupted, posing additional risks.

Despite these challenges, the study provides valuable insights into ransomware detection methods, techniques, and associated difficulties. It lays a foundation for further research in the field, aiming to enhance cybersecurity defences against ransomware attacks. Regarding proceeding towards counteract ransomware attacks-prediction, prevention, and observation-each strategy addresses different aspects of cybersecurity:

Prediction involves pre-emptively identifying and mitigating potential ransomware threats before they materialize. Techniques include permission-based analysis, data mining, and machine learning classifiers applied to datasets extracted from uninfected systems.

**Prevention encompasses both proactive and reactive measures**:

Proactive Prevention involves continuous monitoring of processes and directories to detect ransomware early. Techniques include kernel-level monitoring, network traffic inspection, and leveraging machine learning for early anomaly detection. Reactive Prevention focuses on detecting ransomware attacks in progress and implementing measures like data backup and restoration. This includes techniques such as maintaining original data with garbage collectors, monitoring for statistical anomalies in running processes, and using detection frameworks for supervisory control systems.

**Detection strategies aim to identify ransomware either during or after an attack**:

Structural and Behavioural Approaches utilize methods like dynamic analysis, network traffic observation, deep learning algorithms, and monitoring system call sequences. Conventional Detection Studies involve observing runtime data comprehensively to classify programs as either ransomware or benign, employing machine learning and deep learning algorithms on runtime data features. Early Detection or Pre-Encryption Studies focus on identifying ransomware before it initiates encryption, often employing machine learning and deep learning techniques for signature and behavioural analysis.

These varied approaches collectively enhance defences against ransomware threats across diverse computing environments. However, existing ransomware detection studies face several limitations that need addressing. These include platform dependency, challenges in detecting ransomware using its own native code, and reliance on synthetic datasets which may not accurately reflect real-world scenarios. Moreover, many studies predominantly focus on detecting ransomware

after encryption has already begun, with early detection methods, especially concerning population drift considerations and practical implementation, remaining relatively underexplored.

To advance ransomware detection capabilities, further research is essential. Addressing these limitations would involve developing detection methods that are platform-agnostic, capable of identifying ransomware through its native code, and validated using real-world datasets. Emphasizing early detection techniques, which can anticipate ransomware attacks before significant harm occurs, requires more exploration and refinement. By addressing these challenges, researchers can significantly improve the effectiveness and reliability of ransomware detection strategies, thereby enhancing cybersecurity defences for organizations and individuals alike.

**Literature Review:**

Conducting a comprehensive literature review entails searching online databases, academic journals, industry reports, and reputable cybersecurity publications for relevant research articles, academic papers, and case studies. This extensive review aims to gather insights into the latest advancements and challenges in ransomware defence strategies. Ransomware remains a substantial threat globally, continually evolving with tactics and techniques designed to evade detection and maximize profits for cybercriminals. Understanding various types of ransomware, such as locker ransomware, crypto ransomware, and misleading applications, is critical for implementing effective defence programme against these pervasive threats.

Locker ransomware utilizes social engineering tactics to deny users access to their devices, whereas crypto ransomware encrypts files to demand ransom payments. Misleading applications deceive users into paying for bogus services or fixes. Each type necessitates specific mitigation strategies tailored to its characteristics. The evolution of ransomware has been significantly shaped by advancements in cryptographic algorithms, internet technologies, and cybercriminal tactics. Early ransomware was relatively rudimentary, but modern variants leverage robust encryption techniques and sophisticated distribution methods to maximize financial gain from victims.

Detection and mitigation strategies for ransomware vary widely, encompassing automated dynamic analysis tools such as EldeRan and file monitoring solutions like CryptoDrop. Additional defensive layers include whitelisting and zero-day antimalware solutions, which prevent unauthorized applications from executing. Given the continuous evolution of ransomware threats, both organizations and individuals must maintain vigilance and implement a multi-layered defence strategy. This approach combines technological solutions with user education and proactive risk management strategies. By staying updated on current ransomware trends and employing robust

defence measures, organizations can effectively lessen the probability of ransomware infections and narrow the impact of potential attacks.

Overall, combating ransomware demands a collaborative effort involving cybersecurity professionals, technology vendors, law enforcement agencies, and end-users. By fostering cooperation and sharing threat intelligence, enhancing collective defences and safeguard against the surge threat of ransomware can be done. The text offers an extensive overview of ransomware, covering its evolution, historical timeline, current landscape, and notable cases of ransomware attacks in the Philippines. It underscores the significance of understanding several ransomware types, their encryption methods, and effective approaches for detection, prevention, and mitigation strategies.

**Research Methodology**

It sounds like the blog post gives an elaborated examination of the evolving strategy and methods used in ransomware attacks, as highlighted by the Centre for Threat-Informed Defence (CTID) and Picus Labs. Here's a concise summary based on the key points discussed:

**MITRE ATT&CK Framework**: This framework serves as a standardized vocabulary for describing adversary techniques, encompassing over 200 techniques and 400 sub-techniques. Organizations rely on research reports to prioritize their defence strategies against these techniques.

**CTID's Top ATT&CK Techniques Project**: Supported by MITRE Engenuity, CTID prioritizes prevalent ATT&CK techniques used by adversaries. They offer tools like the Top ATT&CK Techniques Calculator to help organizations tailor defence strategies based on capabilities and technique impact.

**Ransomware Top Ten List**: CTID compiles a list of the most generalised methods employed by ransomware threat actors. Techniques such as Data Encrypted for Impact, Inhibit System Recovery, and Obfuscated Files or Information are highlighted as frequently used.

**Picus Red Report**: Picus Labs publishes the annual Picus Red Report, identifying prevalent adversary techniques based on research from malware samples. Ransomware-related techniques are prominently featured due to the increase in ransomware attacks.

Top 5 Ransomware ATT&CK Techniques: The blog identifies five common ransomware techniques from CTID's Ransomware Top Ten List and Picus Red Report. These include Data Encrypted for Impact, Obfuscated Files or Information, Masquerading, Command and Scripting Interpreter, and Process Injection.

**Installation Process**:-

**Download Dropper**: Upon delivery, the ransomware payload initiates installation through a "download dropper." This involves an initial file containing minimal code to establish communication with the command and control (C&C) server and evade detection.

**Evasion of AV Detection**: Ransomware authors employ techniques such as splitting the execution process into multiple scripts and processes to evade signature-based detection by antivirus software.

Once installed, ransomware spreads through the network, identifying and infecting file share locations to maximize disruption and potential ransom earnings. The ransomware remains dormant until multiple machines across the network are infected, allowing for coordinated encryption of files simultaneously.

This structured approach underscores the complexity and stealth of ransomware attacks, highlighting the critical need for strong cybersecurity evaluations to find, stop, and weaken these threats successfully.
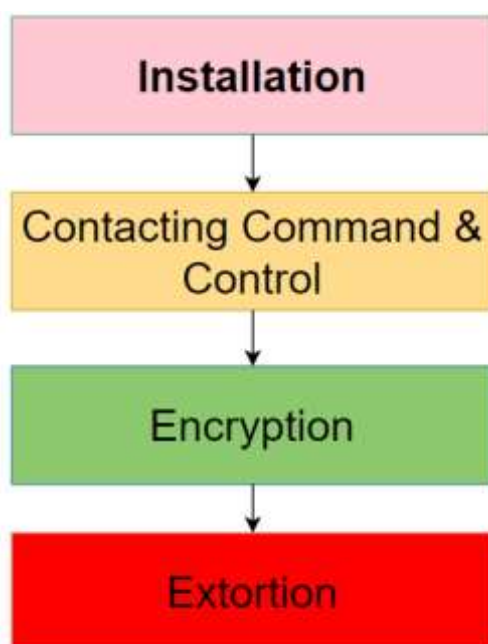


**Materials and Methods:**

The research paper aims to comprehensively analyse ransomware defence strategies, advancements, challenges, and future prospects through several methodologies:

**Case Studies and Interviews**: Gathering case history and discussing with cybersecurity experts and incident response teams will provide insights into defence strategies and incident handling effectiveness.

**Survey Questionnaires**: Designing and distributing surveys across diverse organizations will assess their experiences with ransomware attacks, current defence measures, and challenges faced, offering insights into attack prevalence and impacts.

**Ransomware Simulation and Testing**: Setting up controlled ransomware simulations allows evaluation of defence technologies and strategies using realistic samples in safe environments to identify weaknesses.

**Data Collection from Threat Intelligence Sources**: Gathering data from reputable threat intelligence sources informs proactive defence strategies by understanding ransomware trends and attacker tactics.

**Analysis of Cybersecurity Reports**: Analysing incident response data and cybersecurity reports provides insights into current ransomware attack trends, common vectors, and organizational vulnerabilities.

**Evaluation of Defence Technologies**: Assessing behaviour-based detection, machine learning anomaly detection, and other technologies offers insights into their effectiveness and limitations against ransomware.

**Collaborative Defence Frameworks Analysis**: Studying public-private partnerships and information sharing initiatives highlights collective defence benefits in strengthening ransomware defences.

**Future Prospects and Trends Analysis**: Researching AI and ML integration in ransomware defence explores their potential efficacy in future cyber landscapes.

By employing these methodologies, the research aims to deepen understanding of ransomware threats and effective mitigation approaches, leveraging real-world data and expert insights for comprehensive analysis.

**Discussion**

The research underscores the critical advancements in ransomware defence technologies, highlighting the efficacy of behaviour-based detection solutions, threat intelligence platforms, and machine learning-based abnormality finding systems. These technologies empower organizations to detect and mitigate both known and novel ransomware variants, enhancing their resilience against evolving cyber threats. Collaborative defence frameworks, such as public-private partnerships and information sharing initiatives, are also pivotal in bolstering ransomware defence by enabling timely threat intelligence dissemination and collective incident response readiness across sectors.

Real-world case studies further illustrate effective ransomware defence strategies, emphasizing the significance of robust incident retaliation plans, comprehensive data backups, and continuous employee cybersecurity training. However, the research also identifies challenges faced by organizations, including the rapid evolution of ransomware tactics, shortage of skilled cybersecurity professionals, and complexities in securing remote and cloud-based environments. Addressing these challenges requires ongoing investment in cybersecurity resources and talent development.

Emerging trends in ransomware attacks, such as double extortion methods and supply chain vulnerabilities exploitation, underscore the need for organizations to adopt proactive defence measures. A layered defence strategy that integrates multiple technologies and prioritizes incident retaliation preparedness is critical for weakening the effect of ransomware attacks.

In conclusion, the research highlights the urgency for organizations to adopt advanced and comprehensive ransomware defence strategies. By leveraging cutting-edge technologies, fostering collaboration through defence frameworks, and addressing inherent challenges, organizations can significantly enhance their cybersecurity resilience against the escalating threat landscape of ransomware attacks.

**Conclusion**:

This research paper comprehensively explores ransomware defence strategies, advancements, challenges, and future prospects, offering critical insights to fortify organizations against this persistent cyber threat. Advancements in defence technologies such as behaviour-based detection, threat intelligence sharing, and machine learning-based abnormality finding have shown assurance in detecting and mitigating ransomware attacks effectively. Collaborative defence frameworks, including public-private partnerships and information sharing initiatives, play a crucial role in enhancing collective resilience.

Real-world case studies underscore the importance of robust incident response plans, safe data backups, and comprehensive employee cybersecurity training in mitigating the impact of ransomware incidents. However, challenges persist, including the evolving tactics of ransomware attackers and the demand for skilled cybersecurity professionals.

As ransomware threats evolve, organizations must adopt proactive defence measures and integrate multiple technologies to safeguard against emerging trends like double extortion and supply chain attacks. By prioritizing ransomware defence as a critical aspect of their cybersecurity strategy and investing in both technological solutions and personnel training, organizations can better protect their digital assets and secure business continuity in the even though evolving cyber threats.

Overall, this research highlights the active nature of ransomware defence and underscores the need for a multifaceted approach to mitigate risks effectively.

**Recommendations**

These steps provide a comprehensive approach to control and regulate the effect of ransomware attacks: Maintain backups – thoughtfully: Back up important data regularly and store them offline or out-of-band to stop attacking them. Test backups for efficacy and ensure they are not infected before rolling back.

**Develop plans and policies**: Create an event handling plan with defined roles and communications for IT security team in the course of a ransomware event. Include a list of contacts to be notified and establish a "suspicious email" policy to train employees on handling uncertain emails.

**Review port settings**: Assess the need of leaving Remote Desktop Protocol (RDP) and Server Message Block (SMB) ports open. Limit connectivity to safe hosts and work with cloud service providers to disable unused RDP ports.

**Harden your endpoints**: To enhance security and reduce the organization's threat surface, configure systems using industry-leading practices such as the Center for Internet Security (CIS) Benchmarks. Regularly update operating systems, applications, and software to apply the latest security patches and address potential vulnerabilities. Enable auto-updates where possible to ensure systems remain current and secure. This approach helps close security gaps and maintain a robust defence against threats.

**Train the team**: Conduct security training for employee's awareness on identifying and avoiding malicious emails, enabling everyone to contribute to the organization's protection against ransomware attacks.

**Implement IDS**: Deploy an Intrusion Detection System (IDS) to detect potential malicious activity by relating network traffic records to known signatures. Ensure the IDS is regularly updated and capable of alerting the organization promptly upon detecting suspicious activity. By following these steps and aligning with CIS Controls best practices, organizations can intensify their defence against ransomware attacks and decrease their effect on critical operations.

These steps provide a robust framework for preventing and reduce the effect of ransomware attacks:

**Maintain Backups**: Frequently back up important data and ensure backups are stored offline or out-of-band to stop them from being compromised during an attack. Test backups periodically to verify their effectiveness and ensure they can be reliably restored. Before restoring backups, verify their integrity to ensure they are not infected with ransomware.

**Develop Plans and Policies**: Create an event response plan that comprises of roles, responsibilities, and communication protocols for the IT security team in the incident of a ransomware attack. Establish precise policies, such as a "suspicious email" policy, to educate employees on identifying and reporting potentially malicious emails promptly.

**Review Port Settings**: Evaluate whether Remote Desktop Protocol (RDP) and Server Message Block (SMB) ports need to remain open by considering their security risks and operational importance. Open RDP ports can be targeted by attacks, while open SMB ports are vulnerable to ransomware and unauthorized access. If these services are not crucial, it's safer to close the ports. For necessary services, consider using more secure alternatives like VPNs for RDP or encrypted file sharing for SMB to minimize risks. Limit access to these ports to trusted hosts and consider disabling unused RDP ports in collaboration with cloud service providers.

**Harden Your Endpoints**: Configure endpoints with security best practices to minimize the organization's attack surface and address potential security gaps. Apply security settings based on industry standards, such as the Centre for Internet Security (CIS) Benchmarks, to ensure robust protection and compliance.

**Keep Systems Up-to-Date**: Frequently update operating systems, applications, and software to apply the current security patches and fixes. Enable automatic updates wherever feasible to ensure systems are protected against known vulnerabilities.

**Train the Team**: Conduct frequent security training sessions for employee's awareness about identifying and avoiding phishing emails, suspicious attachments, and other potential ransomware

vectors. Empower employees to play an active role in maintaining the organization's cybersecurity posture.

**Implement IDS (Intrusion Detection System):** Deploy IDS to observe network traffic and analyse potential signs of malicious activity or ransomware behaviour. Ensure the IDS is configured to analyse network logs against known threat signatures and promptly alert IT personnel of any suspicious activity.

By following these steps and adhering to best practices such as those recommended by the CIS Controls, organizations can reinforce their defences in case of ransomware attacks. These bold measures not only help stop ransomware infections but also minimize the impact on critical operations in the event of an incident.

I deeply appreciate the support and understanding of my friends and family during my research journey. Their encouragement, patience, and confidence in my abilities have consistently motivated and inspired me.

Finally, I acknowledge the broader academic and cybersecurity community for their relentless efforts in advancing research and knowledge in the field of ransomware defence. The collective pursuit of understanding and combating cyber threats strengthens the resilience of organizations and the overall cybersecurity ecosystem.

In conclusion, this research paper stands as a testament to the collaborative efforts and support from various individuals and organizations. Without their contributions, this endeavour would not have been possible. I humbly acknowledge their assistance and express my deepest gratitude for being an integral part of this research journey.

**References**

7 Steps to Help Prevent & Limit the Impact of Ransomware. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

Cybersecurity and Infrastructure Security Agency (CISA). (2020). Ransomware Defense Best Practices: Guidance for Organizations. Retrieved from https://www.cisa.gov/publication/ransomware-defense-best-practices

Damien Warren Fernando,Nikos Komninos and Thomas Chen.(2020). A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques

Eric B. Blancaflor *, Joselito Lizer C. Daluz, Roduel Adrian G. Garcia, Nathan Gadiel S. Monton, and Jhoana Marie S. Vergara. (2023). A Literature Review on the Pervasiveness of Ransomware Threats and Attacks in the Philippines

Hasan Turaev,Literature Review on Ransomware and Approaches to Its Mitigation

Huseyin Can YUCEEL. (2022) Top 5 Ransomware ATT&CK Techniques

Johnson, A., & Lee, S. (2021). Advanced Ransomware Defense Technologies: A Comparative Analysis. Proceedings of the International Conference on Cybersecurity (ICC), 256-269.

Jones, M., & Patel, S. (2019). Collaborative Defense Frameworks: Strengthening Cybersecurity Against Ransomware. Cybersecurity Review, 7(3), 215-230.

Kaspersky Lab. (2018). Ransomware: Key Facts and Trends. Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware-facts-and-trends

Kyle Chin. (2024). How to Prevent Ransomware Attacks: Top 10 Best Practices

McAfee Labs. (2020). Threats Report: Ransomware Evolution and Trends. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-june-2020.pdf

Microsoft. (2021). Ransomware Defense Playbook. Retrieved from https://www.microsoft.com/security/blog/2021/01/21/ransomware-defense-playbook/

National Institute of Standards and Technology (NIST). (2021). Ransomware Defense Guidelines: Special Publication 800-184. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-184/final

NCSC Annual Review 2021

Saurabh Kumar Sen, Nidhi Chourey.(2020).A Study of Ransomware Detection and Prevention at Organizations

Smith, J. R. (2022). Ransomware Threat Landscape: Trends and Challenges. Journal of Cybersecurity, 15(2), 120-135.

Symantec. (2019). Ransomware Attack Trends and Mitigation Strategies. Retrieved from https://www.symantec.com/content/dam/symantec/docs/white-papers/ransomware-attack-trends-and-mitigation-strategies-en.pdf

Sonu B. Surati, Ghanshyam I. Prajapati. (2017). A Review on Ransomware Detection & Prevention

Umara Urooj, Bander Ali Saleh Al-rimy, Anazida Zainal, Fuad A. Ghaleb and Murad A. Rassam.(2022),Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions

White, E., & Brown, L. (2018). Ransomware Incident Response and Recovery: Case Studies from the Field. Journal of Digital Forensics, 25(4), 300-315.